Så skyddar du dig mot bedrägeriförsök om dina personuppgifter blivit läckta

Om dina personuppgifter blivit läckta i en attack är du sårbar för bedrägeriförsök. Då är det bra att vara extra vaksam på följande saker.

Granska de som kontaktar dig lite extra

Var uppmärksam på inkommande mejl som känns avvikande- både i jobbet och privat. Det finns avancerad teknik för att förfalska avsändare. Det är därför viktigt att du inte litar blind på de som kontaktar dig, oavsett vilka avsändarna är och hur mycket du litar på dem. Ifrågasätt alltid innehållet i meddelandet.

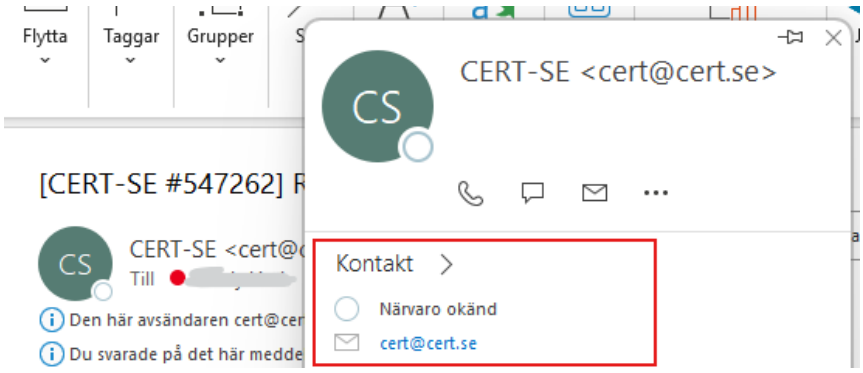
Ett bedrägeriförsök på jobbet kan till exempel se ut så här:

- Din chef ber dig att göra något ovanligt såsom att skapa ett konto eller göra en utbetalning.
- En kollega ber dig att skyndsamt utföra en uppgift – trots att det inte borde finnas orsak till brådska. Till exempel ber de dig att göra en utbetalning eller återställa ett lösenord. De försöker hetsa dig till att agera utan att tänka efter.

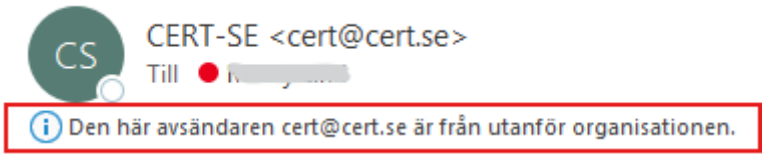
Så här skyddar du dig när du är på jobbet

Många av tipsen här kan du också applicera privat. Liknande funktioner som nämns här brukar finnas i privata verktyg.

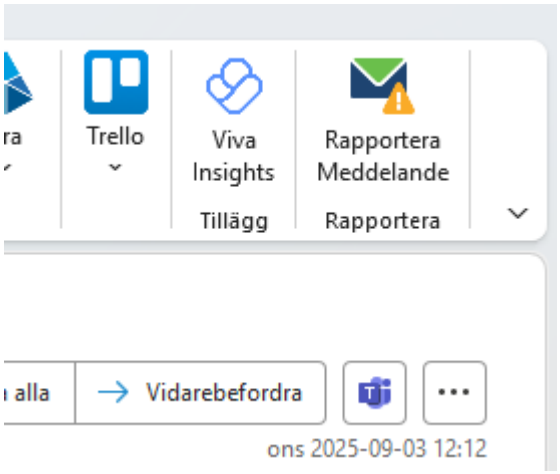
1. **Kontrollera avsändaren**
   Även om namnet ser rätt ut, kan avsändaren vara en helt annan person. Hovra över avsändaren för att öppna upp kontaktkortet helt. Även om du inte ser någon annan information, så ser du hur avsändaradressen ser ut. Ser den korrekt ut? (I det här fallet är det CERT.se, vilket är en ofarlig avsändare efter kontroll).



2. **Var extra vaksam vid externa avsändare**
   Var extra vaksam om mejlet kommer från en extern avsändare. Outlook varnar i så fall med ett meddelande som ser ut så här: ”Den här avsändaren ... är från utanför organisationen”.



3. **Anmäl konstiga mejl så fort som möjligt**
   Det gör du snabbast genom att använda knappen Rapportera meddelande. Den hittar du högst upp till höger i Outlook.



4. **Klicka inte på länkar eller bilagor**
   Klicka inte på länkar eller bilagor om du inte känner igen mottagaren, eller om mejlet ser konstigt ut på något sätt.

5. **Akta dig för telefonbedrägerier**

Var skeptisk mot oväntade telefonsamtal och kontaktförsök. Be att få motringa (alltså lägga på och ringa upp till ett nummer du känner, eller via ett känt växelnummer. Identifiera dig aldrig med exempelvis Bank-ID om det inte är du själv som tagit kontakt.

Klicka inte på länkar eller bilagor i SMS och dylikt.

Anmäl skyndsamt och våga prata om det

Prata med dina kollegor och fråga varandra om råd om något ser konstigt ut. Våga anmäla om du misstänker att du råkat ut för något. Det är lätt att skämmas och känna sig dum om man exempelvis råkat klicka på en länk – men alla kan göra fel. Hör av dig ändå och anmäl det som hänt så snabbt som möjligt till Support Intraservice.

När du inte är på jobbet

Var också uppmärksam på ifall post saknas, om nya bankkonton eller telefonabonnemang du inte känner igen öppnas i ditt namn eller om du får fakturor på varor du inte beställt, och på brev från kreditupplysningsföretag om ansökta krediter som du inte känner igen.

Om du misstänker att dina uppgifter har missbrukats, rapportera detta till polisen omedelbart.

Fler råd

Vill du ha fler handfasta råd kring hur man som privatperson kan agera vid denna typ av incident finns råd till privatpersoner på polisens, MSB:s och Skatteverkets hemsidor. Se länkar för mer information nedan.

Identitetsintrång, skatteverket.se

Identitetsintrång, id-kapning, polisen.se

Digital säkerhet, msb.se

Om du som nuvarande eller tidigare medarbetare i Göteborgs Stad är orolig eller har frågor kan du kontakta den förvaltning eller det bolag som du är eller har varit anställd på. Kontaktuppgifter finns på goteborg.se.